DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
RESPONDING TO BREACH OF PROTECTED HEALTH INFORMATION	**506.03**	**05/03/2011**	**1 of 4**
APPROVED BY:  Director	SUPERSEDES **500.28 05/03/2011**	ORIGINAL ISSUE DATE **05/03/2011**	DISTRIBUTION LEVEL(S) **1**

PURPOSE

1.1 To establish guidance for the workforce members of the Los Angeles County Department of Mental Health (LACDMH) in the event a breach or suspected (possible) breach of Protected Health Information (PHI) is discovered.

1.2 This policy is intended to ensure that LACDMH practices are consistent with the provisions of the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act.

DEFINITION

2.1 **Breach**: The term 'breach' means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security, privacy, or integrity of the health information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. The HITECH Act clarifies that an unauthorized activity compromises the privacy or security of PHI or electronic PHI if it poses a significant risk for financial, reputational, or other harm to the individual.

2.2 **Discovered**: A breach of PHI or electronic PHI will be deemed 'discovered' as of the first day the Department's workforce member knows of the breach, or by exercising reasonable diligence, would or should have known about the breach.

2.3 **Protected Health Information (PHI)**: PHI is individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present, or future payment for health care provided to an individual.

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
RESPONDING TO BREACH OF PROTECTED HEALTH INFORMATION	**506.03**	**05/03/2011**	**2 of 4**

2.4 **Unauthorized Acquisition, Access, or Disclosure**: The terms 'Unauthorized Acquisition', 'Access', or 'Disclosure' of PHI means such was done in a manner not permitted by the HIPAA Privacy Rule or LACDMH policy.

2.5 **Unsecured Protected Health Information**: This concept means PHI that is not secured by a technology or methodology standard (as specified in the guidance issued by the Department of Health and Human Services) that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals.

2.6 **Workforce**: includes employees, volunteers, trainees, and other persons whose work performance is under the direct control of LACDMH, whether they are paid or not.

POLICY

3.1 It is the policy of LACDMH that any staff or manager who becomes aware of a breach of PHI shall immediately notify the LACDMH Privacy Officer and/or Information Security Officer of that non-compliant action.

PROCEDURE

4.1 If a workforce member discovers or becomes aware of a breach or suspected (possible) breach of PHI, he or she must immediately report (immediately means without delay or by the end of one's shift) the incident to his or her supervisor. The supervisor shall report the breach to the Department's Privacy Officer and/or Departmental Information Security Officer (DISO) by telephone or email immediately.

4.1.1 The initial report to the LACDMH Privacy Officer and/or DISO (See Attachment 1 for contact information) should **never include PHI** and only contain the following information:

4.1.1.1 The reporter's name and contact information
4.1.1.2 Short description of the incident
4.1.1.3 Estimated number of affected clients

4.1.2 After the initial report, the workforce member and his/her supervisor must each submit a written report/statement with detailed information (including PHI) to the LACDMH Privacy and/or Information Security Officer **by fax or hand-delivered only** by the end of the next business day.

4.2 The Privacy or Information Security Officer shall make the initial report by telephone call promptly after he or she becomes aware of the breach, followed by a full written report no later than three (3) business days from the date he or she becomes aware of the breach to the Los Angeles County Chief HIPAA Privacy Officer (CHPO) located at 500 West Temple Street, Room 410, Los Angeles, California 90012.

4.3 Following the initial notice of the discovery of a breach, or suspected breach, the LACDMH Privacy and/or Security Officers shall conduct an investigation, including a risk assessment, to determine if the breach is an unsecured or secured breach of PHI and whether the breach is reportable. Either Officer shall forward the determination to CHPO promptly.

4.4 **DOCUMENT RETENTION**

4.4.1 The report and risk assessment of the reported/suspected breach shall be retained for a period of at least six (6) years from the date of its creation.

AUTHORITY

1. 45 C.F.R. Parts 160, 162, and 164
2. 45 C.F.R. Section 164.402 of the Interim Final Rule
3. American Recovery and Reinvestment Act of 2009 Title XIII - Health Information Technology for Economic and Clinical Health Act Section 13402

This policy is meant to co-exist with other breach notification policies and does not substitute or preempt any County policy, Departmental policy, or Board Policy including numbers 3.040 and 6.109.

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
RESPONDING TO BREACH OF PROTECTED HEALTH INFORMATION	**506.03**	**05/03/2011**	**4 of 4**

ATTACHMENT (HYPERLINKED)

1. Privacy and Security Officers' Contact Information

RESPONSIBLE PARTY

LACDMH Compliance, Privacy, and Audit Services Bureau